

一つの非負整数 X をとってきたとき、適当な長さをとると $X \text{ xor } X \text{ xor } \cdots \text{ xor } X = 0$ (演算順序は左から) となるようにできる. よって A は最初から 0 を含むとしてよい.

0 を何回か左からかけることによって添字が置換される回数を調整することができる. よって添字の置換を全て列挙できれば、あとはその xor によって生成される集合の要素数を求めればよい.

xor によって生成されるものの個数は、非負整数を $\{0, 1\}$ 上のベクトル空間ととらえて Gauss の消去法などによってその Rank を求めることで求まる. 添字の置換は、全て列挙すると計算量が破滅するが、ダブリングの要領でやるとうまくいく. 具体的には

- A と A の要素の添字を 1 回置換したものの基底 X_1 をとる.
- X_1 と X_1 の要素の添字を 2 回置換したものの基底 X_2 をとる.
- \dots

などとすればいい.